مجلة الاجتهاد القضائي-المجلد 13– العدد 02 (العدد التسلسلي 27) أكتوبر 2021 (ص ص: 1345 – 1360)
مخبر أثر الاجتهاد القضائي على حركة التشريع - جامعة محمد خيضر بسكرة

الأنظمة القانونية العربية وتحدي التعاون في مواجهة الجرائم المعلوماتية

Arab legal systems and the challenge of cooperation in facing information crimes

ط.د هاني مطر منصور أبوسعود [1]
باحث دكتوراه – مخبر حقوق الانسان والحريات العامة
جامعة عبد الحميد بن باديس- مستغانم (الجزائر)
abusaoud.hani@univ-mosta.dz

د. عباسة طاهر [2]
أستاذ محاضر – مخبر حقوق الانسان والحريات العامة
جامعة عبد الحميد بن باديس- مستغانم (الجزائر)
Taher.droit@hotmail.fr

تاريخ الارسال:	تاريخ القبول:	تاريخ النشر
01 أفريل 2021	30 جويلية 2021	31 أكتوبر 2021

الملخص:

لقد ألقت الثورة المعلوماتية بضلالها على قوانين العقوبات لمختلف الدول بالتصدي للجانب السلبي منها مع ضرورة مراعاة تحقيق هدفين أساسيين هما، عدم تفويت الفرصة في الاستفادة من تطور التقنية المعلوماتية ومن ناحية أخرى ضرورة حماية الأقتصاد والأمن الوطني وحقوق وحريات الأفراد من جراء العمل غير الشرعي لهذه التقنية، والملاحظ في هذا الصدد أنه كلما كان الأعتماد أكبر على التقنية المعلوماتية كلما كانت الحاجة أكثر إلحاحا لوضع نصوص قانونية لحماية هذه المعلوماتية وفي هذا الصدد كان لابد للمشرعين العرب أن يعملوا على تطوير منظومتهم القانونية بما يتوافق مع التطور التكنولوجي الهائل خالقين قواعد قانونية لمكافحة الجريمة المعلوماتية.

الكلمات المفتاحية: الجرائم المعلوماتية، حماية المعلومات، جرائم الحاسب الآلي، التعاون العربي.

Abstract:

The information revolution has cast a shadow over the penal laws of various countries by addressing the negative side of them, with the need to take into account the achievement of the two main objectives: not to miss the opportunity to benefit from the development of information technology and on the other hand the need to protect the economy and national security and the rights and freedoms of individuals due to the illegal work of this technology, In this regard, the greater the reliance on information technology, the more urgent the need to develop legal texts to protect this information. In this regard, it was necessary for Arab lawmakers to work to develop their legal system in accordance with the And technological innovation, creating legal rules against cybercrime.

Key words: *Information crimes, information protection, computer crimes,Arab cooperation.*

[1] المؤلف المرسل: ط. د هاني مطر منصور أبوسعود ـــــ ***Email : hanimatar20@gmail.com***

مقدمة:

على الرغم من الأهمية العظيمة والمزايا الهائلة التي حققتها الثورة التكنولوجية والقفزة الحضارية النوعية لحياة الأفراد والدول بفضل التطور العلمي في شتى ميادين الحياة وإعتماد القطاعات المختلفة في وقتنا الحالي في أداء أعمالها بشكل أساسي على أستخدام الأنظمة المعلوماتية نظرا لما تتميز به من عنصري السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها، إلا أن هذا التطور والرواج في قطاع المعلومات في كل الدول العربية صاحبته جملة من الإنعكاسات السلبية والخطيرة مهدت لظهور العديد من الممارسات الإجرامية الجديدة في العالم الإفتراضي، حيث يطلق عليها تسمية الجرائم المستحدثة والتي تتنوع ويتزايد عددها يوما بعد يوم فهي متعددة ومتجددة وقابلة لظهور أنماط أخرى وفقا للتطورات التكنولوجية، ومن هنا يتبين لنا أن الجرائم المعلوماتية والجرائم الإلكترونية هي نتاج للثورة التكنولوجية العملاقة في القرن العشرين.

مما حذا بالدول العربية إلى محاولة إيجاد سبل تشريعية وإجرائية ناجعة لمواجهة هذا النوع من الجرائم المستحدثة، عبر تشريعاتها الوطنية من أجل مواجهة كل من تسول له نفسه خرق الآداب العامة بأعمال غير مشروعة، ومن ذلك الجرائم المرتكبة ضد المعلومات بإختلاف طريق إرتكابها.

وفي هذا السياق سنرى كيف حاربت المنظومة القانونية العربية عبر التشريعات الوطنية هذا النوع من الجرائم بالنظر إلى التشريعات العربية التي أُقرت في مجال مكافحة الجرائم المعلوماتية والإلكترونية، وابراز مدى التعاون العربي في مجال الحماية المعلوماتية ومواجهة الجرائم ذات الطابع المعلوماتي والإلكتروني، وفي هذا الصدد تطرقنا لتجربة عدد من الدول العربية (الامارات، الكويت، الاردن، الجزائر).

وعليه نطرح الإشكالية التالية: هل عملت الدول العربية على مكافحة الجرائم المعلوماتية وعالجت القصور التشريعي في قوانينها بما يحقق إقامة آليات للتعاون؟.

ومنها يمكن طرح الاسئلة الفرعية التالية:

- كيف عملت الدول العربية على مواجهة الجرائم المعلوماتية؟
- هل واكب المشرع الجزائري التطور الحاصل في قوانين مكافحة الجرائم المعلوماتية؟
- هل التعاون العربي واقعيا كافي لمواجة الجرائم المعلوماتية؟

ولمحاولة الإلمام بجميع جوانب الدراسة، والإجابة عن الإشكالية المطروحة أعلاه تم اتباع المنهج التحليلي لتحليل النصوص القانونية التي جاءت بها التشريعات العربية لمواجهة الجرائم المعلوماتية.

ولغرض دراسة الموضوع قسمناه إلى مبحثين تعرفنا في الأول على التشريعات العربية الصادرة في مجال مكافحة الجرائم المستحدثة وتناولنا في المبحث الثاني التعاون العربي في مواجهة الجرائم المعلوماتية.

المبحث الأول: المنظومة القانونية العربية لحماية المعلومات

لم يكن المشرع العربي غافلا عما يقع من إعتداءات على أفراد المجتمع سواء أكان على أنفسهم أو أموالهم عن طريق إستخدام التقنية التكنولوجية، لذلك عمل جاهدا على مواكبة تلك التشريعات التي صدرت في العديد من دول العالم لتكافح هذا النمط من الإجرام المستحدث، ولكنه يبدو جليا أنه لم تسعى بعض الدول العربية لوضع قوانين خاصة بجرائم المعلومات وذلك نتيجة تأخر دخول خدمات الانترنت لهذه الدول، فحين بدا إستخدام الأنترنت بها ظهرت جرائم مصاحبة لبداية عمل هذه الخدمة، وقد اختلفت وجهات النظر هل تكفي القوانين التقليدية والقواعد العامة لاستيعاب جرائم المعلومات والأنترنت، أم أن هذه الدول بحاجة إلى قوانين جديدة خاصة بالجرائم المعلوماتية، هذا ما دعانا إلى دراسة المنظومة القانونية العربية عبر مطلبين، خصصنا الأول للتشريعات العربية الصادرة في مجال مكافحة الجرائم المعلوماتية، أما الثاني فخصصناه حصرا لدراسة للتشريع الجزائري في مواجهة الجرائم المعلوماتية.

المطلب الأول: التشريعات العربية في مجال مكافحة الجرائم المعلوماتية

لقد كان دور المشرع في دول الخليج العربي الأبرز في هذا المجال، حيث سلك الطريق الذي شقه أغلب المشرعين في الدول لإصدار القوانين التي تواجهه الجرائم المعلوماتية وحماية برامج الحاسب الألي وتطبيقاته ضد أي إعتداء يقع عليها.

1- الأمارات العربية المتحدة:

جاء القانون الإتحادي في شأن مكافحة جرائم تقنية المعلومات كخطوه أولى لحماية سرية الإتصالات بين الأفراد، وصدر قانون مؤسسة الأمارات للإتصالات رقم 1 لسنة 1991، حيث تم وصف هذا القانون بالمرونة مما سهل على الجهة المختصة تقديم مرتكبي الأفعال الواقعة على تقنية المعلومات للعدالة، وأمام عجز هذا القانون على حماية قطاع الإتصالات من الإعتداءات الواقعة عليه[1]، فقد صدر مرسوم بقانون إتحادي رقم 3 لسنة 2003 بشأن تنظيم قطاع الإتصالات حيث جاءت المادة 71 منه على العقوبة التي تترتب على مخالفة أحكام هذا القانون، كما جاء نص المادة 72 لينص على بعض الأفعال التي إعتبرها القانون جرائم معلوماتية ليصنف إستغلال أجهزة الأتصال في الإساءة أو الإزعاج او إيذاء مشاعر الأخرين أو

القيام بتوزيع أي أتصال أو رسالة هاتفية، ضمن الأفعال التي إعتبرها القانون جرائم معلوماتية[2].

وتطويرا للقانونين السابقين أصدر المشرع الإماراتي قانونين بشأن جرائم المعلوماتية في سنة 2006 الأول والمنشور في الجريدة الرسمية في العدد رقم 442 بتاريخ 2006/01/30 بمسمى قانون إتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات بالأمارات، حيث ضم 26 مادة.

والثاني في عام 2012 حيث صدر القانون رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، وقد ضم 51 مادة، جاء في المادة الأولى منه التعريف ب 18 مصطلح مستخدم في هذا القانون أو يدخل ضمن الجرائم، وما له علاقة بها كتعريف "المحتوى، المعلومات الإلكترونية، الشبكة المعلوماتية، الموقع الإلكتروني، وسيلة تقنية المعلومات، البيانات الحكومية" وغيرها من المصطلحات[3].

وفي المادة الثانية نص القانون على التعريف بالجرائم والسلوكيات غير القانونية في البيئة الإلكترونية وعلى شبكة الأنترنت وأنظمة المعلومات الآلية، حيث حددت العقوبات لكل حالة، وهي ما بين العقوبات المادية التي تتراوح ما بين 100 الف درهم و3 ملايين درهم اماراتي، وبين العقوبات الجسدية المتمثلة بالحبس ما بين السجن المؤقت، والحبس بين ستة أشهر إلى خمس سنوات، كما أشار القانون في مادته 16 إلى أشد عقوبات الحبس التي تصل إلى 10 سنوات إذا كان التهديد بارتكاب جناية أو المساس بالشرف والإعتبار[4].

أما المواد الأخيرة في هذا القانون فتوضح طرق تنفيذه والإشارة إلى القوانين المشابهة وطرق التعامل معها، وقد جاءت المادة 50 لتعلن عن إلغاء القانون سابق الذكر القانون الإتحادي رقم 2 لسنة 2006.

2- الكويت: قانون مكافحة جرائم تقنية المعلومات:

قامت دولة الكويت في سنة 2015 بإعداد قانون خاص بمكافحة جرائم تقنية المعلومات، والذي جاء بعد أهم نصين قانونيين في مجال تكنولوجيا المعلومات وهما القانون رقم 20 لسنة 2014 في شان المعاملات الإلكترونية، والقانون رقم 37 لسنة 2014 بإنشاء هيئة تنظيم الإتصالات وتقنية المعلومات، حيث شمل الأخير على إحدى وتسعون مادة ويحتوي على أحد عشر فصلا، فضلاً عن الفصل الثاني عشر الذي يضم أحكاما ختامية[5].

ليكون هذا القانون الموسوم بقانون 63 لسنة 2015 في شان مكافحة جرائم تقنية المعلومات والصادر في تاريخ 2015/07/07 أول نص مفصل ومعالج للجرائم المعلوماتية حيث جاء

القانون مكون من فصلين ضما 21 مادة عالجت مختلف الجوانب القانونية والاجرائية في مجال مكافحة الجرائم المعلوماتية.

شمل الفصل الأول على التعريفات ليفصل في 16 مصطلح مستخدم في هذا القانون، ومن بين المصطلحات (البيانات الإلكترونية، النظام الإلكتروني المؤتمت، نظام المعالجة الإلكترونية للبيانات، الشبكة المعلوماتية، الجريمة المعلوماتية،...)[6].

وجاء الفصل الثاني بعنوان الجرائم والعقوبات ليفصل في 20 مادة مختلف أنواع الجرائم والسلوكيات والتعديات التي تعتبر مخالفة للقانون وحددت عقوبات كل فعل من هذه الأفعال، وقد حددها هذا القانون بنوعين من العقوبات المادية متمثله في غرامات تتراوح ما بين 500 دينار كويتي و50 ألف دينار كويتي، والعقوبات الجسدية ممثله في الحبس بمدة ما بين 6 أشهر إلى 10 سنوات[7].

3- الأردن: قانون جرائم أنظمة المعلومات

قدم المشرع الأردني في سنة 2010 قانون جرائم أنظمة المعلومات وإعتبره في العنوان قانون مؤقت رقم 30، حيث ضم القانون 17 مادة وجاء في مادته الأولي تسمية القانون، وجاءت مادته الثانية للتعريف بالمصطلحات المقدمة والمستعملة في هذا القانون ومنها (نظام المعلومات الموقع الإلكتروني) ومصطلحات أخرى، وإبتداء من المادة الثالثة يبدأ عرض الجرائم والأفعال غير القانونية وعرض العقوبات الخاصة بكل حالة، وهي عقوبات بين المادية والجسدية تتراوح بين 100 دينار و2000 دينار أردني، إضافة إلى الحبس ما بين أسبوع إلى سنتين والأعمال الشاقة.

ومن بين الجرائم المشار إليها في هذا القانون نجد الدخول إلى المواقع الإلكترونية وإفشاء وإتلاف أو حجب معلومات في نظم المعلومات، الإلتقاط والتعرض والتنصت على مراسلات الشبكات العنكبوتية وإستخدام نظم المعلومات للأغراض المخلة بالأدارب والترويج للأفعال غير القانونية، ليصل القانون إلى المادة 12 لتحديد مهام بعض العاملين في المجال من ضباط العدالة، والمدعي العام، كذلك ابراز مهام المحاكم المختصة في هذا القانون، أما المادة 15 فحدد فيها تشديد العقوبات في حالات تكرار أي من الجرائم المنصوص عليها فيه[8].

أنه وبالرغم من هذه التشريعات العربية لمكافحة جرائم المعلوماتية، الظاهر جليا ان المشرعين العرب اتجهوا إلى الاكتفاء بتعديل القوانين العقابية أو الجزائية من خلال إضافة بعض النصوص التي تتعلق بالجريمة المعلوماتية، ومنها على سبيل المثال الإتجاه الذي أخذ به المشرع العماني(قبل أن يقوم بإصدار قانون الجريمة المعلوماتية)، فبالرجوع إلى احكام قانون الجزاء العماني الصادر بموجب المرسوم السلطاني رقم 2001/72 والذي كان تعديلا للقانون رقم

1974/7 والذي يعتبر أول قانون عربي يتطرق إلى الإجرام المعلوماتي، فقد أضاف الفصل الثاني مكرر إلى الفصل السابع والذي جاء بعنون (جرائم الحاسب الآلي) حيث أشتمل هذا الفصل على خمس مواد تم إستحداثها، وهي تعبر عن إرادة المشرع ورغبته في مواكبة التطورات السريعة والهائلة لتكنولوجيا شبكات الإتصال والمعلومات[9].

وحسما لهذا النزاع فقد قامت أغلب الدول العربية بتطبيق قانون العقوبات وادرجت الأحكام المستجدة الخاصة بجرائم الأنترنت تحت هذا القانون بالقياس على الجرائم التقليدية وذلك عند وجود التوافق والتشابه بين المقيس والمقاس عليه، ومن هذه الدول دولة مصر مثلا التي عملت عمل فرنسا فطبقت قانون الصحافة والنشر على قضايا الأنترنت على إعتبارها أنها وثيقة الصلة بها، وأنها أنسب القوانين لهذه الجريمة، وكذلك قامت البحرين بتطبيق قانون العقوبات على الجرائم المعلوماتية وجرائم الأنترنت[10].

المطلب الثاني: التشريع الجزائري في مجال مكافحة الجرائم المعلوماتية

واكب المشرع الجزائري مختلف التطورات التشريعية التي تم سنها من أجل تنظيم المعاملات التي تتم من خلال الوسائط الإلكترونية، وإيماناً منه بأن الجزائر ليست بمعزل عن التطورات الإجرامية التي تحدث في العالم، بداء إهتمامه في مجال تكنولوجيا المعلومات حديثا ومحدودا فكانت محاولاته في الحد من الظاهرة المستحدثة على النحو التالي:

- القانون رقم 97-10 لسنة 1997 المتعلق بحماية حقوق المؤلف والحقوق المجاورة له كان أول قانون للمشرع الجزائري في مجال حماية المعلومات[11].
- القانون 04-15 والمؤرخ في 2004/11/10 والذي تضمن تعديل قانون العقوبات بالنص على الأفعال الماسة بأنظمة المعالجة الإلكترونية للمعطيات، في القسم السابع مكرر 3 في المواد 394 مكرر إلى 394 مكرر 4 حيث جاء هذا القسم بثمان مواد وصفت عددا من السلوكيات والتعديات على نظم المعلومات إضافة إلى العقوبات المترتبة على كل واحدة منها، وبهذا يمكن تقسيم العقوبات المسلطة في قانون العقوبات الجزائري ضد مختلف التعديات على النظم الآلية للمعلومات إلى قسمين، عقوبات بسيطة عندما لا تقترن الجرائم بأي ظرف من ظروف التشديد بسبب عدم إلحاقها لخسائر للأفراد أو ضد النظم في حد ذاتها، كما قد تكون مشددة عندما تقترن الجرائم بظرف من ظروف التشديد حيث حددت هذه الظروف في إلحاقها لخسائر أو مساسها بالمعلومات أو النظم ذات المصلحة العامة أو الهيئات الحكومية أو النظام العام[12]، إلا أن البعض قد إشار إلى أن المشرع الجزائري من خلال نصوص هذا القانون فقد ركز على الإعتداءات التي تمس الأنظمة المعلوماتية في حين أغفل على تلك الإعتداءات الماسة بمنتوجات الأعلام الآلي والمتمثلة بالتزوير المعلوماتي[13].

• القانون09-04 والصادر في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، حيث يعتبر هذا القانون نطاقا شاملا في مجال مكافحة الجرائم المرتكبة عبر الأنترنت، فشمل على ستة فصول و19 مادة جاءت بتجريم الأفعال المخالفة للقانون والتي ترتكب عبر وسائل الإتصال عامة وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الأنترنت وعلى كل تقنية تظهر مستقبلا[14].

• إضافة إلى التشريع الذي جاء به المشرع الجزائري في مجال الوقاية من هذه الجرائم المستحدثة نجد أنه كرس إيضا من خلال القانون رقم 09-04 مكافحة هذه الجرائم عبر إنشاء هيئات متخصصة منها:

○الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، والتي أنشئت بموجب المادة 13 من القانون 09-04 وتمت المصادقة على انشائها بالمرسوم الرئاسي 16-261 المؤرخ في 2015/10/18 المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الأعلام والإتصال ومكافحتها.

○الهيئات القضائية المتخصصة، نشئت بموجب القانون رقم 04-14 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية وتختص هذه الأقطاب بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات حسب المواد 37 و40 و329 قانون الإجراءات الجزائية، وتتميز بإختصاص إقليمي واسع حسب المرسوم التنفيذي رقم 348-06 المؤرخ في 2006/10/05 وحسب المادة 15 من القانون رقم 09-04، والشيء الملاحظ أن المشرع الجزائري قد وسع من صلاحيات الضبطية القضائية عند معاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بتمديد الأختصاص المحلي إلى كامل الإقليم الوطني مع إمكانية الانتقال لتفتيش الأماكن السكنية وغير السكنة بإذن من وكيل الجمهورية.

○تكريس المشرع الجزائري إيضا مبدأ التعاون الدولي والمساعدة القضائية كما ورد في المادة 16 من القانون رقم 09-04 في إطار (جمع وتبادل المعلومات في الشكل الإلكتروني، أستعمال وسائل الإتصال السريعة مثل البريد الإلكتروني والفاكس في حالة مستعجلة، القيام بالإجراءات التحفظية حسب الاتفاقيات الدولية ومبدأ المعاملة بالمثل)، كما أورد المشرع إيضا قيودا على طلبات المساعدة القضائية الدولية حسب المادة 18 من نفس القانون إذا كانت تمس بالسيادة الوطنية أو النظام العام والإلتزام بالسرية في الطلبات المقيدة بذلك وإستعمالها للغرض المطلوب.

ومن صور هذا التعاون نجد على سبيل المثال مذكرة التفاهم في إطار مكافحة القرصنة والتزوير بالكمبيوتر بشكل مشترك من قبل الديوان الوطني لحقوق المؤلف وشركة مايكروسوفت، وفعلا لوحظ أثر هذه المذكرة على أرض الواقع في مجال مكافحة قرصنة البرمجيات وفي عمليات السيطرة على برامج مايكروسوفت المستخدمة في الشركات والإدارات[15].

المبحث الثاني: التعاون العربي في مواجهة الجرائم المعلوماتية

للتعاون العربي أهمية بارزة في مجال مكافحة الجريمة، وذلك بعد ان أصبحت الأخيرة تتخطى حدود الدول والتي لم تقف حائلا إمامها وابرز وأوضح مثال على ذلك الجرائم المعلوماتية، وعلى الرغم من كون التعاون والتنسيق العربي يتقدم بشكل مشجع بشان مكافحة الجريمة بصورة عامة، إلا أنه لم يصل إلى درجة تسمح بإيجاد نظام جنائي عربي فعال يوازي التقدم التكنولوجي الذي يشهده العالم، حيث ان الوسائل والتدابير المتخذة في هذا المجال وعلى الرغم من جديتها إلا أنها لا ترتقي إلى مستوى التحدي الذي تفرضه الجريمة العابرة لحدود الدولة[16]، ولذلك قسمنا هذا المبحث إلى مطلبين تناولنا في الأول واقع التعاون العربي، وفي الثاني اشكاليات التعاون العربي.

المطلب الأول: واقع التعاون العربي في مجال مكافحة الجرائم المعلوماتية

بالرغم من القصور التشريعي في ملاحقة السلوك الضار والخطر المتعلق بالجرائم المعلوماتية إلا أنه كان هناك محاولات جادة لتنظيم ذلك، ومن هذه المحاولات ما بذلته الجمعية المصرية للقانون الجنائي بعقد مؤتمرها السادس في القاهرة في الفترة 25 وحتي 28 اكتوبر 1993 وناقش موضوع جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات من خلال الدراسات والأبحاث المقدمة من الباحثين والتي دارت حول تحديد أنواع الجرائم المختلفة المتعلقة بنظم المعلومات من إعتداء مادي على الأجهزة وأدوات الكمبيوتر، وقد بينت تلك الأبحاث والدراسات صعوبة إكتشاف جرائم نظم المعلومات وإثباتها وأكدت على ضرورة تدريب رجال الشرطة القضائية ورجال التحقيق ورجال القضاء، وفي نهاية المؤتمر فقد تمكن المؤتمرون من تجريم الأفعال المتعلقة بالكمبيوتر والتوصية باتخاذ التدابير والإجراءات التشريعية اللازمة لمكافحة هذه الجرائم[17].

أما جامعة الدول العربية فقد إعتمدت عبر الأمانة العامة لمجلس وزراء العدل العرب ما سمي بالقانون العربي الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، أين تم إعتماده من قبل مجلس العدل العرب في دورته التاسعة عشر بالقرار رقم (495/د19/ المؤرخ 2003/10/08) ويعد هذا القانون أبرز الجهود العربية المبذولة في مجال الحماية من الجرائم

المعلوماتية من الناحية التشريعية، وقد تضمن هذا القانون 27 مادة موزعة على أربعة أبواب يعالج الباب الأول الجرائم المعلوماتية، والتي تم النص عليها في المواد من 3 إلى 22 ومن أهمها:

- جريمة الدخول بغير حق إلى موقع أو نظام معلوماتي، مع تشديد العقوبة إذا كان بغرض إلغاء أو إتلاف أو إعادة نشر بيانات أو معلومات شخصية.
- جريمة تزوير المستندات المعالجة في نظام معلوماتي وإستعماله.
- جريمة الإدخال الذي من شأنه إيقاف الشبكة المعلوماتية عن العمل، أو إتلاف البرامج أو البيانات فيها.
- جريمة التنصت دون وجه حق على ما هو مرسل عن طريق الشبكة المعلوماتية.
- الجرائم المخلة بالآداب العامة عبر الشبكة المعلوماتية.

وتناول الباب الثاني التجارة والمعاملات الإلكترونية، أما الباب الثالث فقد تناول حماية حقوق المؤلف عبر الوسائط الإلكترونية في حين عالج الباب الرابع الإجراءات المتعلقة بالجريمة المعلوماتية.

وإن كان القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها جاء موفقا إلى حد ما في أحكامه الموضوعية حيث شملت بياناً لأهم الجرائم التي يمكن أن ترتكب في مجال الأنظمة المعلوماتية، إلا أنه يؤخذ عليه خلوه من الأحكام الإجرائية الضرورية لملاحقة هذه الجرائم، فلم يتعرض لمسألة الإختصاص القضائي بشكل واضح ولم يشر إلى إخضاع البيانات والمعلومات لإجراءات التفتيش والضبط، ولم يتعرض كذلك لمفهوم الدليل التقني وشروطه وحجيته[18].

ومن هذه المحاولات أيضا ما صدر كذلك عن مجلس وزراء الداخلية العرب بإصداره قانون نموذجي حول جرائم الأنترنت على صورة مشروع، تمت المصادقة علية في سنة 2004 والذي كان ثمرة الجهد المشترك حيث تم إعداده من قبل لجنة مشتركة بين المكتب التنفيذي لمؤتمر وزراء الداخلية العرب والمكتب التنفيذي لمجلس وزراء العدل العرب في نطاق الأمانة العامة لجامعة الدول العربية، بعد أن تبين أن كلاهما قد قدم مشروعا بهذا الخصوص، حيث تم إقراره بوصفة منهجا إسترشاديا يلتزم به المشرع الوطني عند إعداد تشريع في الجرائم المعلوماتية، وأُقر هذا القانون بصورته النهائية في عدد 27 مادة[19].

ولم يكن المشروع المقدم من طرف وزراء الداخلية العرب هو المرجعية الوحيدة التي تأثر بها المشرع العربي في سعيه إلى تنظيم النظم المعلوماتية وحمايتها قانونينا، بل إن هناك تشريعات أوروبية وأمريكية سابقة في هذا المشروع تركت بصماتها على قوانين الأنترنت في الدول العربية، كما أن الاتفاقية الموضوعية في أطار النظام القانوني الإقليمي الأوروبي حول

الأنترنت أي اتفاقية بودابيست سنة 2001 كانت هي الأخرى ذات تأثير ملموس على القوانين العربية[20].

ووصولا إلى عام 2010 تم عقد الأتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة بتاريخ 21 ديسمبر 2010 وذلك لتحديد الجرائم المتعلقة بالإرهاب ومرتكبيه بواسطة تقنية المعلومات، أما مؤتمر أبوظبي المنعقد بتاريخ 15-16 ماي 2017 تحت عنوان المؤتمر الدولي لتجريم الإرهاب الإلكتروني فقد أكد على إيجاد أطار تشريعي دولي شامل للإرهاب الإلكتروني، ووضع إستراتيجية للتصدي له[21]، وتدريجيا ومع التطور التكنولوجي كان لا بد من حتمية التعاون العربي في مكافحة الجريمة المعلوماتية وهذا لعدة مبررات نذكر منها:

- أن أي دولة مهما بلغت درجة قوتها وصلابتها لا تستغني عن الدخول في علاقات تعاون متبادلة مع غيرها من الدول، خاصة وأن جهودها الداخلية لمكافحة الجرائم لا تعد كافية لمنع الجريمة أو تقليصها وذلك لسبب التقدم التكنولوجي مما يساعد على ظهور أنماط جديدة للجريمة.

- الجرائم المعلوماتية جرائم غير أقليمية في أغلب الاحيان، مما يؤدي إلى توزيع أركانها على عدة دول، كما أن أدلة إثباتها يسهل طمثها ومحوها مما يجعل هناك صعوبة قائمة ضد القوانين التقليدية في مواجهة هذا النوع من الجرائم، وهذا ما يتطلب أجهزة تعاون تعمل على مستويات حكومية.

- ان هذا التعاون العربي يعتبر خطوه على طريق تدويل القانون الجنائي، وذلك أن ثمة قواعد موضوعية إجرائية متقاربيه بين التشريعات، فتقارب هذه التشريعات يجعل من الحديث عن تدويل القانون الجنائي أمرا قابلا للتحقيق.

- انه يعتبر من قبيل التدابير المانعة من ارتكاب الجريمة لأن المجرم سيجد نفسه محاط بسياج مانعة من الافلات من العقاب والمسئولية عن الجريمة التي ارتكبها، أو من العقوبة التي حكم بها[22].

المطلب الثاني: إشكاليات التعاون العربي

بالرغم من الجهود المبذولة والتشريعات القانونية للحد من الجرائم المعلوماتية وحماية أمن المعلومات وبالرغم من المناداة بضرورة التعاون العربي في مجال مكافحة الجريمة المعلوماتية والذي أصبح مطلبا تسعى إلى تحقيقه أغلب الدول العربية، إلا أنه هناك العديد من الصعوبات والمعوقات التي تقف دون تحقيقه وتجعله صعب المنال، نوجزها فيما يلي:

1- القصور التشريعي في مواجهة الجرائم المعلوماتية:

لقد وجدت العديد من الثغرات القانونية التي تعتبر قصور تشريعي لمواجهة الجرائم المستحدثة(المعلوماتية)، وبالتالي عدم أمكانية إحتضان القانون الجنائي لهذه الطائفة من الجرائم، فإذا كانت التشريعات العقابية العربية قد تناولت الجرائم التقليدية التي تقع على الأشخاص أو الأموال وجرمتها بوضع العقاب على كل من يقوم بارتكابها، إلا أنها(النصوص العقابية التقليدية) قد لا تطال معظم الإنتهاكات الإلكترونية الرقمية بالتجريم لأسباب قد تعود إلى ما تتمتع به هذه الجرائم من طبيعة خاصة تميزها عن غيرها من الجرائم من ناحية الأركان والمحل[23].

2- صعوبة إثبات الجرائم المعلوماتية واكتشافها:

من إشكاليات الجريمة المعلوماتية أنها تتميز في أكثر صورها بأنها مستتره وخفيه ولا يلاحظها المجني عليه غالبا أو يدري بوقوعها، فهي غالبا تكتشف بمحض الصدفة، ولذلك توصف بالجريمة غير المرئية، فالفعل الأجرامي في هذه الجرائم ليس له اثار مادية، فلا يوجد أدلة قولية أو مادية أو حالات تلبس يمكن إدراكها بالحواس، حيث أن الدليل في هذه الجرائم يكون في صورة نبضات إلكترونية غير محسوسة ويحاول المجرم في هذه الجريمة قدر الامكان إعاقة الوصول إلى الدليل بشتى الوسائل[24]، ولهذا فأن الإثبات في الجريمة المعلوماتية يصاحبه العديد من العوائق التي تقف حائلا دون اتمامه ومنها:

- ان الأثار التي تخفيها الجريمة المعلوماتية ذات طبيعة غير مادية، وهذا ما يمثل صعوبة في إثبات هذا النوع من الجرائم، ولكن هذا لا يعني أن الجرائم المعلوماتية لا تتخلف عنها أثار مادية بشكل مطلق.
- أن شبكة الأنترنت ليس لها حدود دولية فهي لا تعترف بالحدود التقليدية بين الدول، كما انها ليست مملوكة لأحد، وبالتالي لا يوجد جهاز رقابي عليها ولا سلطة مركزية تتحكم فيها، فالأنترنت ظاهرة دولية تنعدم مركزيتها وتتساوى أمامها الدول الكبيرة والصغيرة.
- ضخامة كم البيانات والمعلومات والتي بحاجة إلى فحص ودراسة لاستخلاص دليل الجريمة منها، ولذلك على السلطات القائمة بالتحقيق ان لا تتمتع بالخبرة والمعرفة الفنية في مجال الحاسب الالي فقط بل وانما لابد ان تمتلك هذه السلطات أيضا القدرة على فحص الكم الهائل من المعلومات والبيانات.

3- عدم وجود نموذج موحد للنشاط الإجرامي:

بالنظر إلى الأنظمة القانونية لمواجهة الجرائم المعلوماتية في الكثير من الدول يتضح عدم وجود أتفاق مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الأنترنت الواجب تجريمها، فما يكون مباحا في أحد الأنظمة قد يكون مجرما وغير مباح في نظام أخر.

4- مشكلة الإختصاص في الجرائم المعلوماتية:

تعد الجرائم المعلوماتية والجرائم المتعلقة بالأنترنت من أكبر الجرائم التي تثير مسالة الإختصاص المحلي أو الدولي ولا توجد أي مشكلة بالنسبة للإختصاص على المستوى الوطني حيث يتم الرجوع إلى المعايير المحددة قانونا لذلك، لكن المشكلة تثار بالنسبة للإختصاص الدولي حيث الأختلاف في التشريعات القانونية والتي قد تنجم عنها تنازع في الإختصاص بين الدول بالنسبة للجرائم المعلوماتية، التي تتميز بكونها عابرة للحدود[25].

5- إختلاف النظم القانونية الإجرائية:

إذ بسبب هذا الإختلاف قد تكون هناك طرق للتحري والتحقيق والمحاكمة التي تثبت فعاليتها في دولة ما، قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها كما هو الحال مثلا بالنسبة للمراقبة الإلكترونية، فإذا ما إعتبرت أن طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى، بالإضافة إلى أنه قد لا تسمح دولة ما باستخدام دليل إثبات جرى جمعه بطرق ترى هذه الدول أنها طرق غير مشروعة[26].

في الحقيقة إن المصلحة المشتركة للدول العربية تقتضي البحث عن الوسائل التي تساعد في التغلب على هذه الصعوبات وإيجاد تعاون عربي حقيقي يتفق مع طبيعة هذا النوع المستحدث من الجرائم للتخفيف من الفوارق بين الأنظمة القانونية العقابية الداخلية.

خاتمة:

ما يتضح لنا أن الجرائم المعلوماتية لها طبيعتها الخاصة والمتميزة ذلك لعدة إعتبارات منها طبيعة المحل المعلوماتي في الجريمة المعلوماتية وحداثة نظام الحاسب الآلي والتقنية العالية التي يستخدمها المجرم في الجرائم المعلوماتية، بالإضافة إلى التحديات التي فرضت على الجهات الخاصة بوضع القوانين وإنفاذها، وأمام مشكلة من المشكلات التي أفرزتها ثورة الاتصالات فبقدر ما قدمته هذه الثورة من تسهيلات للأفراد والمجتمعات بقدر ما زعزعت سكينتهم بهذا النوع الجديد من الجرائم.

ومن جانب أخر فأن القانون الجنائي لا يتطور دائما بنفس السرعة التي تتطور بها الحياة والتكنولوجيا أو مهارة الذهن البشري، بالإضافة إلى مبدأ الشرعية الجنائية حيث

يفترض عدم جواز التجريم والعقاب عند إنتفاء النص، سواء أكان ذلك يتعلق بشرعية أو قانونية الجرائم، والذي يعني أن كل واقعة لا يمكن أن تعد جريمة ما لم يقرر القانون ذلك، وعليه نخلص إلى النتائج التالية:

النتائج:

- بالنظر إلى المنظومة القانونية العربية فمن الواضح أن هناك فراغا تشريعيا عربيا في مجال حماية النظم المعلوماتية ومكافحة الجرائم المعلوماتية.
- القوانين الجنائية والموضوعية والإجرائية التقليدية العربية مازالت قاصرة ولا تفي لمواجهة هذا النوع من الجرائم.
- الدول العربية الواردة في الدراسة سعت جاهدة لتطوير منظومتها التشريعة وإصدار قوانين خاصة بالاتصالات والجرائم الالكترونية والمعلوماتية لتتوائم مع التطور التكنولوجي الحديث، إلا أن أغلب الدول الأخرى عملت على تعديل قوانينها الجنائية فقط بما يتوافق مع التطور التكنولوجي وأضافة بعض المواد الجديدة التي لها علاقة بمكافحة الجرائم المعلوماتية.
- إن المشرع الجزائري عمل جاهد على مواكبة التطور الحاصل على المستوى التشريعي الدولي فيما يخص مكافحة الجرائم المعلوماتية عبر أصدار العديد من القوانين الخاصة بمكافحة الجرائم المعلوماتية.
- إن التعاون العربي المشترك في مجال مكافحة الجرائم المعلوماتية لم يرتقى إلى المستوى المطلوب.

وعلى هذا الأساس يمكن تقديم التوصيات التالية:

التوصيات:

- تعزيز الأطار التشريعي العربي عبر أصدار إتفاقيات عربية مشتركة خاصة بمكافحة الجرائم المعلوماتية مع النص على تجريمها في التشريعات الوطنية.
- إرساء قواعد تعاون عربي فاعل وحقيقي في مواجهة الجرائم المعلوماتية وإستخدام تقنيات التحقيق الخاصة الشيء الذي يخفف من غلو واختلاف النظم القانونية والإجرائية.
- العمل على تبادل المعلومات بين الأجهزة الأمنية المعنية بمواجهة الجرائم المعلوماتية وإنشاء خلايا عمل مشتركة تعمل على رصد مخاطر الجرائم المعلوماتية ومحاربتها، والعمل على تجسيدها من الناحية التطبيقية بتكوين فرق من الضبطية القضائية والقضاة المتخصصين في هذا النوع من الجرائم ومدها بكافة الوسائل المادية والتقنية اللازمة لأداء عملها.
- لفت انتباه مستخدمي تكنولوجيا التقنية العالية إلى خطورة الجريمة المعلوماتية وطرق الحماية منها من خلال ورش العمل التعريفية والأعلامية.

الهوامش:

[1] – لينا محمد الاسدي، مدى فاعلية احكام القانون الجنائي في مكافحة الجريمة المعلوماتية دراسة مقارنة، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان الأردن، 2015، ص 67-68.

[2] – أنظر المادة 71 و72 من المرسوم بقانون اتحادي رقم 03 لعام 2003 الامارات العربية المتحدة، بشأن تنظيم قطاع الإتصالات الصادر بتاريخ 2003/11/15، (يعاقب بالحبس مدة لا تزيد عن سنتين وبالغرامة التي لا تقل عن خمسون الف درهم ولا تزيد عن مليون درهم أو بأحدى هاتين العقوبتين: 1- كل من يباشر أيا من الأنشطة المنظمة دون أن يكون مرخصا له أو معفيا من ضرورة الحصول على ترخيص وفقا لاحكام القانون.2- كل من يقوم متعمدا بتغيير أو اتلاف أو اخفاء أية وثيقة أو معلومة يطلبها المجلس أو الهيئة بموجب أحكام القانون...).

[3] – أنظر المادة الأولى من القانون رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات الاماراتي، المنشور بالجريدة الرسمية عدد 540، بتاريخ 26-08-2012.

[4] – بلال بن جامع، الجرائم المعلوماتية على شبكة الانترنت، أطروحة دكتوراه، معهد علم المكتبات والتوثيق، جامعة قسنطينة 2 عبد الحميد مهري 2016-2017، ص 200-201.

[5] – أنظر القانون رقم 37 لعام 2014 بشأن إنشاء هيئة تنظيم الإتصالات، الصادر عن مجلس الوزراء الكويتي، والمنشور بالجريدة الرسمية العدد 1184 السنة الستون الموافق 2014/05/18.

[6] – أنظر المادة الأولى من القانون رقم 63 لعام 2015 في شأن مكافحة جرائم تقنية المعلومات، الصادر عن مجلس الوزراء الكويتي، بتاريخ 2015/7/7 والمنشور بالجريدة الرسمية العدد 1244 في 2015/07/12.

[7] – بلال بن جامع، المرجع السابق، ص 205.

[8] – انظر المواد من 1 إلى 17 من قانون جرائم نظم المعلومات المؤقت الأردني لعام 2010.

[9] – لينا محمد الاسدي، المرجع السابق، ص 71-72.

[10] – عبد العزيز بن جرم الله آل جابر، جرائم الانترنت وعقوبتها وفق نظام مكافحة الجرائم المعلوماتية السعودي، الطبعة الأولى، دار الكتاب الجامعي للنشر والتوزيع، مصر،2017، ص265-266.

[11] – محمد ممدوح بدير، مكافحة الجريمة المعلوماتية عبر شبكات الانترنت والاستدلال كوسيلة لإثبات الجريمة المرتكبة عبر الانترنت دراسة مقارنة، الطبعة الأولى، مركز الدراسات العربية للنشر والتوزيع، مصر،2019، ص 148.

[12] – انظر المادة 394 مكرر من قانون العقوبات الجزائري المعدل بالقرار رقم 04-15 لعام 2004.

[13] – بلال بن جامع، المرجع السابق، ص 211.

[14] – محمد ممدوح بدير، المرجع السابق، ص 162.

[15] – عبد الرحمن نشادي، الجرائم المعلوماتية في وسائل الاتصال الحديثة، أطروحة دكتوراه، كلية علوم الاتصال، جامعة الجزائر3، 2016-2017، ص 202-203.

[16] – لينا محمد الاسدي، المرجع السابق، ص 251-252.

[17] – عبد العزيز بن جرم الله آل جابر، المرجع السابق، ص 269-270.

[18] – سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2012-2013، ص 85-86.

[19]– عادل عبد العال أبراهيم خراسي، إشكاليات التعاون الدولي في مكافحة الجريمة المعلوماتية وسبل التغلب عليها، الطبعة الأولى، دار الجامعة الجديدة للنشر، مصر، 2015، ص88.

[20]– يوسف حسن يوسف، الجرائم الدولية للأنترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، مصر، 2001، ص 264.

[21]– حسين عبد علي عيسى، هه لاله محمد تقي محمد امين، التعاون الدولي في مواجهة الإرهاب الإلكتروني، مجلة دراسات قانونية وسياسية، مركز الدراسات القانونية والسياسية، كلية الحقوق جامعة السليمانية، العراق، العدد 11 نيسان 2018، ص 38.

[22]– عادل عبد العال ابراهيم خراسي، المرجع السابق، ص 16–17.

[23]– لينا محمد الأسدي، المرجع السابق، ص 237–238.

[24]– عادل عبد العال ابراهيم خراسي، المرجع السابق، ص53.

[25]– محمد احمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الالكترونية، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة، بجاية الجزائر، المجلد 14 العدد 02–2016، ص61.

[26]– محمد ممدوح بدير، المرجع السابق، ص190.